




County of Los Angeles CHIEF EXECUTIVE OFFICE

Kenneth Hahn Hall of Administration
500 West Temple Street, Room 713, Los Angeles, California 90012
(213) 974-1101
<http://ceo.lacounty.gov>

SACHI A. HAMAI
Chief Executive Officer

November 16, 2015

To: Supervisor Michael D. Antonovich , Mayor
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe

From: Sachi A. Hamai 
Chief Executive Officer

Board of Supervisors
HILDA L. SOLIS
First District

MARK RIDLEY-THOMAS
Second District

SHEILA KUEHL
Third District

DON KNABE
Fourth District

MICHAEL D. ANTONOVICH
Fifth District

FEASIBILITY OF CONDUCTING ANNUAL INFORMATION TECHNOLOGY (IT) AND SECURITY POLICY AUDITS (ITEM NO. 8, AGENDA OF JULY 14, 2015)

On July 14, 2015, on a motion from Supervisor Mark Ridley-Thomas, the Board of Supervisors (Board) directed the Auditor-Controller (A-C), in coordination with the Interim Chief Executive Officer (CEO), to report back in 60 days on the feasibility of conducting Information Technology (IT) and Security Policy Reviews of every County department, including the CEO and Executive Office of the Board of Supervisors, on an annual basis.

In addition, the Board instructed the CEO to require any department or office with IT security vulnerabilities, as identified by the A-C, to submit detailed reports to the Board, A-C and the Chief Information Office (CIO), County Chief Information Security Officer (CISO) every 90 days on the progress being made to correct each security vulnerability and the steps being taken to prevent further future problems until each vulnerability is fully corrected.

Feasibility of Conducting Annual IT and Security Policy Reviews

Fundamental to the achievement of reasonable IT security assurance are the staff resources and technical tools already funded within County departments to develop and maintain their IT security infrastructure. Departments' IT security experts should be regularly reviewing the strength of their IT security methods to ensure compliance with Board IT policies and prepare for evolving security threats. However, it is important to continually identify IT vulnerabilities through independent certifications of compliance with County IT policies and it is equally essential to constantly improve strong IT security defenses within the County's larger IT environment. While it is feasible to

"To Enrich Lives Through Effective And Caring Service"

**Please Conserve Paper – This Document and Copies are Two-Sided
Intra-County Correspondence Sent Electronically Only**

conduct annual IT policy audits of every County department, due to departmental size variances and system configuration complexities, we estimate the annual cost to be significant. Preliminarily, the A-C developed five scenarios (Attachment 1) that estimates the cost of performing IT policy audits based on varying frequencies. However, before recommending any of the five scenarios or other alternatives, we believe it is critical to expand the A-C's current risk assessments to incorporate each department's current level of knowledge and their monitoring efforts to ensure compliance with the IT policies. I have directed the A-C, to immediately contract with an outside IT security assessment expert to assist with this risk assessment, which will include reviews of written policies, procedures, practices, and interviews with departmental IT staff and management. These assessments will assist the A-C to incorporate additional elements into their current risk assessments and may identify potential departmental IT vulnerabilities that can be incorporated into the County's coordinated IT security program.

The A-C will have an agreement established as soon as feasible with the assessments being completed on a flow basis. We have included \$300,000 in the Fiscal Year (FY) 2015-16 Supplemental Budget to begin this effort.

Benefits of Annual IT Policy Audits

Annual IT policy audits will provide independent oversight to help identify potential vulnerabilities and ensure timely corrective action to protect IT equipment and sensitive data. The audits may also cause departmental staff to be more vigilant in their adherence with IT policies, which may also better insulate the County from costly data breaches.

As previously mentioned, annual audits would be costly and until new staff could be hired and trained, existing audit resources would need to be redirected from their current and planned assignments to complete the IT audits. Redirecting staff would also limit the A-C's resources to perform other critical unplanned audits directed by the Board, (e.g., LA County Fairplex Review, the Office of Management and Budget Uniform Guidance Implementation, etc.).

Given the importance of this effort, the involved departments will continue to assess the effectiveness of the County's IT security strategy and will come back to the Board during the FY 2016-17 budget process with additional recommendations.

Audit Corrective Action Plan

A key element of every audit report includes the department's Corrective Action Plan (CAP) on identified deficiencies or anomalies. This CAP describes specific accomplishments and progress being made to correct deficiencies and vulnerabilities

Board of Supervisors
November 16, 2015
Page 3

identified by the A-C and are submitted on a flow basis. Effective immediately, all IT security policy deficiencies identified as a result of an audit review, as prepared by the A-C, CIO, or third party expert, will require the department to submit a detailed CAP to the Board, A-C and the CIO within 90 days. Further, a CAP progress status report will be required every 90-days thereafter to address corrective actions being taken for each IT security vulnerability identified, and the steps taken to prevent further future problems until each issue is fully corrected.

If you have any questions or need additional information, please contact me, or your staff may contact Jim Jones at (213) 974-8355 or via e-mail at jjones@ceo.lacounty.gov

SAH:JJ:SK
BM:ef

Attachment

c: Executive Office, Board of Supervisors
Auditor-Controller
Chief Information Office
County Counsel
Internal Services
Audit Committee

Auditor-Controller
Information Technology and Security Policy Audit Scenarios

November 2015

		Scenario 1		Scenario 2		Scenario 3		Scenario 4		Scenario 5	
		<i>Annual Audit Cycle for All Departments (Board Directive)</i>		<i>Annual Audits for High Risk Depts 3 Year Cycle for Med Risk 5 Year Cycle for Low Risk Annual Follow-up Reviews for All</i>		<i>2 Year Cycle High Risk 4 Year Cycle Medium Risk 5 Year Cycle Low Risk Annual Follow-ups for All</i>		<i>3 Year Cycle for High Risk 5 Year Cycle for Med/Low Risk Annual Follow-ups for High Risk Biennial Follow-ups Med/Low Risk</i>		<i>5 Year Cycle for All Departments Biennial Follow-ups All</i>	
Position	Cost Per Position ¹	No. of Positions	Annual Cost	No. of Positions	Annual Cost	No. of Positions	Annual Cost	No. of Positions	Annual Cost	No. of Positions	Annual Cost
Chief Accountant-Auditor	\$ 211,699	2	\$ 423,398	2	\$ 423,398	2	\$ 423,398	1	\$ 211,699	1	\$ 211,699
Principal Accountant-Auditor	\$ 191,915	6	\$ 1,151,487	4	\$ 767,658	4	\$ 767,658	3	\$ 575,744	3	\$ 575,744
Senior Accountant-Auditor	\$ 137,622	12	\$ 1,651,467	8	\$ 1,100,978	7	\$ 963,356	5	\$ 688,111	4	\$ 550,489
Intermediate Accountant-Auditor	\$ 115,831	28	\$ 3,243,260	25	\$ 2,895,768	17	\$ 1,969,122	14	\$ 1,621,630	10	\$ 1,158,307
Totals		48	\$ 6,469,613	39	\$ 5,187,803	30	\$ 4,123,535	23	\$ 3,097,184	18	\$ 2,496,239
Current Audit Resources ²		(8)	\$ 1,218,265	(8)	\$ 1,218,265	(8)	\$ 1,218,265	(8)	\$ 1,218,265	(8)	\$ 1,218,265
Additional Resources Needed		40	\$ 5,251,348	31	\$ 3,969,538	22	\$ 2,905,270	15	\$ 1,878,919	10	\$ 1,277,974
Estimated Intrafund Transfers Needed			\$ 2,716,214		\$ 2,223,296		\$ 1,518,217		\$ 996,054		\$ 637,701
Estimate Net County Cost Needed			\$ 2,535,133		\$ 1,746,242		\$ 1,387,053		\$ 882,866		\$ 640,273

¹ Cost is based on fiscal year 2015-16 Salary & Employee Benefits billing rates, multiplied by 1,776 productive work hours; and does not include Services & Supplies costs which would be negligible for Scenarios 4 and 5. Scenarios 1 through 3 would likely require additional office space costs which we are unable to estimate at this time.

² Resources are funded as part of the Audit Division's annual budget process, and were redirected from existing resources and audits of other critical County operations. Current resources in the IT audit function include: 1 CAA, 2 PAA's, 2 SAA's and 3 IAA's/AA's.

